Curriculum Design Requirements and Challenges for the First Bachelor's Degree on IoT in the US

Kemal Akkaya

Curriculum Design Requirements and Challenges for the first Bachelor's Degree on IoT in the US

Kemal Akkaya

Department of Electrical and Computer Engineering
Florida International University
Miami, FL 33174 USA
kakkaya@fiu.edu

Abstract. Internet of Things (IoT) devices have become part of our lives through their roles in smart and connected living. As they are increasingly deployed in various industries and residential areas, they are now readily accessible to the end users who need to manage them on a daily basis. However, management of these devices includes many aspects such as hardware troubleshooting, operating systems updates, security configuration, connectivity maintenance and scripting, etc. Given the complexities of these tasks, there is a need to educate and train technical people who will eventually form a new workforce to handle these issues on behalf of the ordinary users. This brings the need for a new IoT related curriculum that will serve to undergraduate students to acquire the above skills. In this paper, we present the first undergrad IoT curriculum in the US offered by Florida International University (FIU) by discussing the requirements and challenges. We explain how this new curriculum addresses the key aspects of IoT technologies and opportunities that come with the proposed IoT degree. We also highlight other related issues regarding the focus of this type of degrees and interdisciplinary aspects with other academic units and industry.

Keywords: IoT · IoT curriculum · IoT education · IoT challenges.

1   Introduction

Motivated with the proliferation of smart, low-cost and small devices, there is a growing trend towards the development of smart buildings, cities, and infrastructures in order to make our lives more efficient, cleaner, safer and less costly than before [1–5]. These devices are now widely referred to as Internet of things (IoT), which became part of our lives. Examples of these IoT devices include smart sensors, thermostats, meters, phones, tablets, cameras, wearable technologies (e.g., glasses, watches), and cars that are currently ubiquitous [6–8]. These IoT devices have typically computation, communication, sensing, and storage capabilities and have been the focus of a great deal of research in the last

several years. Such research activities range from the hardware/software charac-
teristics [9, 10] of these individual devices to their deployment challenges in the
development of smart spaces and infrastructures [11, 12].

With such developments, IoT applications started to dominate our lives in
our homes, schools, workplaces. It can be said that while the term IoT was
coined in 1999 by Kevin Ashton [13], we have started to witness the IoT era
only after 2010s with the maturation of the IoT technology. Specifically, with
the introduction of smart home devices such as Nest thermostat, Apple HomeKit,
Amazon Alexa, etc. as well as the penetration of smart phones, we have seen
a dramatic increase in IoT device deployment in every domain and hence the
number of IoT devices that are deployed worldwide surpassed the number of
people connected to Internet. According to a new Gartner report, almost 5 billion
IoT devices are in use worldwide as of Dec. 2019 [14]. The application categories
of these devices are listed in Table 1. The table indicates that there are numerous
market segments where IoT devices are increasingly used. In fact, it is predicted
that "the combined markets of IoT will grow to about $520 billion in 2021, more
than double the $235 billion spent in 2017 [15].

Table 1. IoT Device count by billions in various segments (Source Gartner).

Segment	2019	2020
Utilities	1.17	1.37
Government	0.53	0.70
Building Automation	0.31	0.44
Physical Security	0.95	1.09
Manufacturing	0.40	0.49
Automotive	0.36	0.47
Healthcare Providers	0.28	0.36
Retail & Wholesale Trade	0.36	0.44
Information	0.37	0.37
Transportation	0.07	0.08
Total	4.81	5.81

These developments indicate that the demand for the deployment of IoT will
only grove further in the upcoming decade which will eventually require creating
a new workforce to manage these devices. This is because, from their mainte-
nance/updates to integration with IT, and from their security to programming,
there will be a lot of technical tasks to be handled when IoT devices are used.
This ultimately means, millions of new jobs will be created in the upcoming
decade to fill the gap in the market. Indeed, International Data Corporation has
predicted that IoT will be a $7 trillion industry by 2020 [16]. Currently, there
is already a growing job market in IoT in regards to managing IoT data on the
cloud, analyzing security and privacy issues, understanding networking issues
surrounding IoT systems (i.e., 4/5G, WiFi, Zigbee, Bluetooth), programming

server side for IoT using *Node.js* and using machine learning to do predictions with IoT data [17].

We argue that most of the aforementioned jobs and skills are specific to IoT domain and independent from IT or computer science/engineer related jobs. This means they will require special training in the domain of IoT. Therefore, current curriculum in computer science or engineering will not be able to address this need given that their focus is not on IoT. While some of the jobs can still be done using general computer science or engineering skills, there is a need to design specific courses that will get into the realm of IoT to understand the context, requirements and challenges. Given the increasing demand and broad concepts under IoT, addressing this need with one or more elective courses will not be the ideal solution. While it is certainly helpful to have certificates or training programs such as Intel's IoT curriculum [18] or Stanford's IoT certificate for graduates [19], the training and education should be made more accessible to a broader audience including college students and professionals. Otherwise, companies will still need to train their employees in IoT domain to equip them with the emerging skills which may cost them more money.

In this paper, we present the first IoT Bachelor's degree in the US to address the above needs and challenges. We first motivate the specific need and thus the required type of curriculum and then we explain the details of the curriculum structure created in the Department of Electrical and Computer Engineering at Florida International University (FIU). We share our challenges when the degree is to be offered as a technology degree rather than engineering. We provide discussions on how and where to create such type of degrees in the future depending on the need.

This paper is organized as follows: In the next section, we motivate the need for a new IoT technology degree at the undergraduate level. Section 3 explains the pillars of the proposed IoT degree. Section 4 is dedicated to overall IoT map in the proposed curriculum. Section 5 presents other related issues and Section 6 concludes the paper.

2   Where is the Need?

One of the challenges that comes with proposing a new degree is whether it is different than the existing degrees and it will survive in the long run. This was very much true for IoT since it includes many components that are already being taught under Computer Science or Engineering programs. In this section, we explain how the proposed IoT degree is different and what kind of gap it would fill.

2.1   IoT vs Computer Science/Engineering

IoT is mainly about engineering so a new engineering degree on IoT would be a special case of either Computer Science or Computer Engineering depending on the focus of the degree. For instance, if software is the main focus, then Computer

Science courses could be expanded to cover IoT software development. Indeed, there is already courses on various universities that teach Android programming, iOS programming, IoT data collection via Cloud Computing, IoT data analytics, IoT security, etc. On the other hand, if the focus is more on hardware level, then Computer Engineering courses can be expanded to focus on microcontrollers for IoT, embedded programming, sensors for IoT, IoT communications, etc.

Nevertheless, current jobs in IoT domain require a comprehensive skill set that forces companies to train their computer science or computer engineering workforce in one of the above aspects of IoT as their training is not comprehensive enough to cover all of the desirable IoT skills. Thus, a new IoT Engineering degree would address these needs which would be a mix of computer science or engineering programs with some special IoT courses. Such IoT undergrad programs are indeed emerging in China [20–22] and becoming popular among the new college students.

2.2 IoT vs IT

Even if there is a justification for a new engineering degree, the booming applications of IoT showed that the need is not just at the engineering level. This is because, these devices are now used in many domains by non-technical people as a lot of homes/companies/cities are maintaining IoT devices and infrastructure. Thus, there is a different need in terms of their maintenance and management. Specifically, we need technical people to deploy, manage, secure, update, troubleshoot IoT devices and networks for sustainable operations.

This need is similar to the case with Information Technology (IT) related jobs in early 2000s. Basically, as Internet was penetrating through every domain, industries, organizations and schools started to deploy computers and a network infrastructure to manage their websites and store their data. However, this necessitated technical specialists who can manage these computers and networks which basically included maintenance, software updates, security, troubleshooting, upgrades, configuration, etc. Obviously, Computer Science graduates were capable of handling these tasks but they would be considered over-qualified for these tasks and thus they were not able to fill this gap. Therefore, a lot of Computer Science departments started to offer a new degree called IT or Information Systems (IS) which aimed at producing workforces that can handle IT maintenance/management. These programs spread to every College in the US and eventually attracted many students who were not necessarily strong in Math and programming but still have a genuine interest in technology. IT graduates filled the gap in the workforce and are still in high demand today.

This led us to think in the same way and offer IoT as a technology degree that will fill an important gap in the IoT workforce. In this way, the engineers or scientists who came out of computer science or engineering programs can still be employed in engineering related jobs for IoT (i.e., design and development of IoT devices or IoT networks) but there will be a separate pipeline for IoT management/maintenance jobs that will suit the students who are interested in technology.

3 IoT Technology Degree Curriculum

With the given motivation for a technology degree in IoT, under the Electrical and Computer Engineering at FIU, a new IoT BS degree is designed [23] in 2018. This is known to be the first IoT degree at the undergraduate level in the US. In this section, we explain the core elements of this proposed IoT degree and provide examples for the new courses.

3.1 University Core Requirements

Before discussing the IoT-related core courses, we first briefly mention the university core requirements for our degree. As the core courses that will be taken mainly within the first two years, we ensured that the prerequisites are different than engineering programs in terms of Math requirements. Specifically, Calculus or Discrete Math are not required as part of this new degree since it focuses less on Math but more on technology. However, we expect students to take some basic programming and data analysis courses which are widely available in many colleges.

3.2 Four Pillars of IoT

We consider 4 major pillars to base the proposed degree after the university core classes are completed. Basically, this corresponds to roughly the last two years of the program. These pillars are based on the main elements of an IoT device as shown in Fig. 1. We discuss each in details below.

IoT Device Components
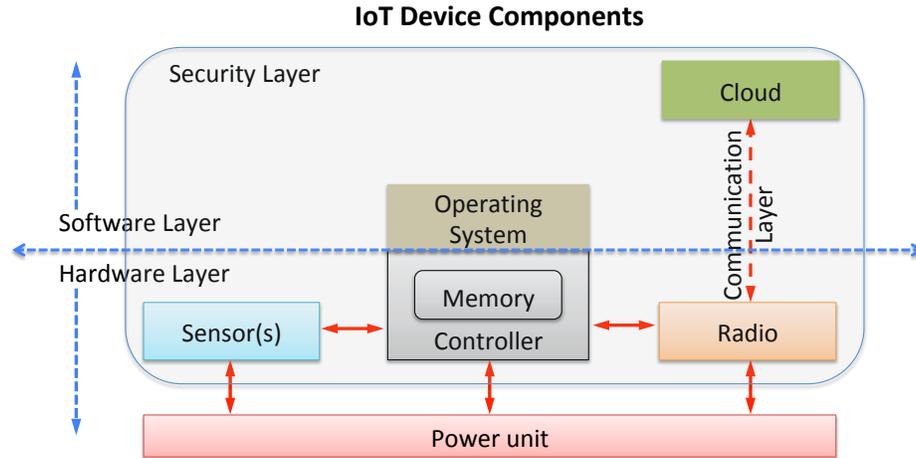
Fig. 1. Main components and related layers of an IoT device.

Hardware Hardware components are very critical for understanding IoT. Basically, these components refer to microprocessor/controller, sensors and memory which are very different than traditional ones used in computers due to resource constraints in IoT devices. Specifically, due to their size and cost requirements, the hardware is specially designed for IoT and it is a constant area of research that evolves every year. The hardware classes should cover all these aspects in a comprehensive manner. For instance, there needs to be a course focusing on IoT microprocessors or microcontollers and teach their features within a comparative framework with others. Memory and storage units could be under another separate course. Finally, sensors augmented to IoT devices forms a whole different world that includes their design, calibration and management. A course on sensors should teach how these sensors are built and what their features are.

Obviously, in order to teach these courses, the students should first acquire a background on digital electronics and computer design. Therefore, we also introduce new courses on these topics that need to be crafted in such a way that they will not require Calculus. This is one of the challenges as most of the existing computer engineering courses require Calculus and Circuits courses as prerequisites. To this end, we propose two new courses that offers such a background: First, we designed a new course on Digital Electronics and Circuits which focuses solely on digital aspects and eliminates any analog elements which require more advanced Math. Second, we designed a course that will teach basic computer architecture by considering the IoT device architectures. These two courses are kept as mandatory before any other hardware related courses could be taken.

Software The software aspects of IoT is pretty broad that spans from programming languages, operating systems to data management via cloud computing. Depending on the program's focus, the set of the software related courses could be adjusted. The major component is programming with IoT devices. To this end, we consider two major programming languages, namely Android Programming and C. As Java is already expected as part of the university core Math requirements, building Android skills on top of Java will be easier. Most of the Computer Science programs offer mobile programming courses and they can be easily adapted for the IoT degree. In our proposed program, since it was under Electrical and Computer Engineering, we offered only C programming which is instrumental in many embedded programming environments. For programs where Python is also offered, this can also be a good match for the Software component of IoT degree.

Apart from programming, there are other elements such as Operating Systems and data management. In our degree, we included an Operating Systems course as part of the curriculum although it is generic Operating Systems class. This will enable understanding the underlying operating systems for IoT devices such as Linux, Android, and other specialized real-time operating systems. For instance, widely used Raspberry PI devices [24] utilize Linux which makes it convenient to run many applications written in diverse programming languages.

Per the data management, there is a huge space that relates to cloud management as most of the IoT data is stored in cloud servers through special platforms. Teaching tools to store, retrieve and process IoT data would definitely be relevant. In our proposed curriculum, there is no mandatory course on it but we plan to offer electives as the program becomes more mature.

Communications Another important aspect of IoT is their ability to communicate their data via a communication environment. In many cases, this communication is done via wireless channel so it is imperative to teach the wireless concepts before explaining how special IoT data collection protocols work. Current IoT applications heavily utilize WiFi, Bluetooth, Zigbee, Zwave, LoRa and 4/5G standards. Therefore, the students first need to understand the wireless communication basics. To this end, we designed a new course that will teach Wireless Communications which is a simplified version of Digital Communications course in Computer Engineering departments. This course explain the nature of radio signals, communication propagation, channel interference and modulation techniques without getting into their design principles.

Once these concepts are taught, the next step is to give some background on networking, mainly TCP/IP. As IoT devices heavily rely on IP, it is necessary to teach the students how these devices get connected to Internet and what services each layer of the TCP/IP protocol stack provides. Finally, with all of these background, we offer how the existing wireless standards work briefly in another course on IoT Protocols and Standards. This course aims to show the configuration for these protocols and weighs the different options to be deployed under various application requirements. It also offers a layered network architecture which introduces gateways and their communication protocols with the cloud through widely used communication standards for IoT such as Message Queue Telemetry Transport (MQTT) [25] or Constrained Application Protocol (CoAP) [26].

Cybersecurity The final aspect of an IoT curriculum would be to focus on the security and privacy aspects of these technologies as they pose several critical issues that are probably the most important for the consumers and other stakeholders. To this end, our proposed curriculum first offers a fundamentals course on security which teaches very basics of cybersecurity elements and services. This course does not have any prerequisites other than College Algebra and is typically offered as soon as the students enter the program.

After this introduction, the students are offered a new course on Security of IoT. This course focuses on the threats and vulnerabilities of various IoT devices and networks and includes hands-on activities to be applied on actual IoT devices. This is one of the most attractive courses of the program given that it is new and providing hands-on learning experience.

Under this pillar, there are other aspects that can be taught under elective courses. For instance, we designed another new course on IoT Privacy which solely focuses on privacy of the users and shows how these devices may become

vulnerable to privacy leakage. Another course, we designed was on IoT Forensics. This course is also elective but focuses on the forensics tools on various IoT hardware. Another potential course on this pillar could be IoT Ethics and Compliance that trains students on compliance issues when data are collected from IoT devices.

4   Proposed IoT Program Map

After providing the main elements of the proposed IoT curriculum, in this section we outline a sample map of the courses and prerequisites as well as providing other related information.

4.1   Prerequisites

Our degree is a 120 credits hours degree with 40 credits as part of the core IoT while the remaining are allocated for the university core courses and electives. Specifically, 50 credits are coming from university core requirements while 40 credits will be IoT core courses. The remaining 30 credits are electives. Among these 30 credits, 9 credits should be from the home department, 9 credits from other engineering electives while the remaining 12 credits can be from any other college. These credits can be adjusted depending on the needs and availability of electives. A sample flow chart for all courses in the curriculum is shown in Fig. 2.
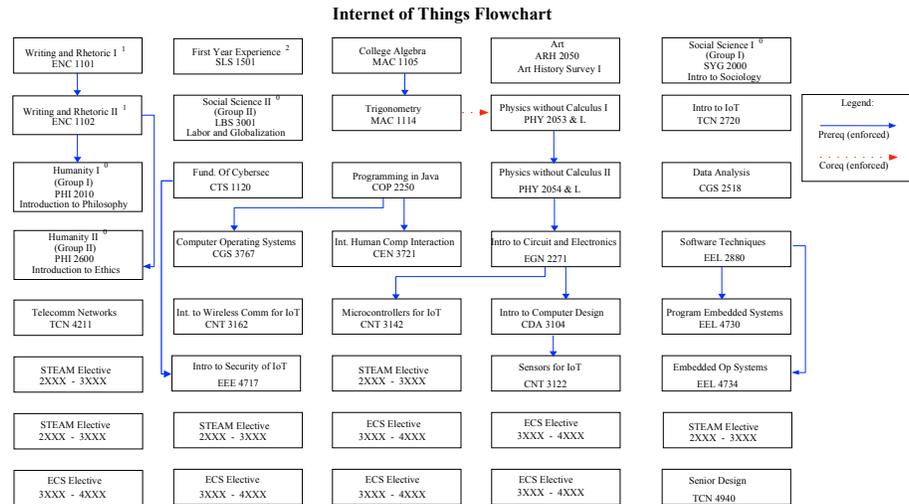
Fig. 2. A sample flowchart for the courses in the proposed IoT program at FIU.

4.2   Online vs Onsite

One of the other challenge in designing such a new IoT degree is whether to offer it online. This comes from the motivation that most of the students who will be attracted to the program are from professionals in other disciplines or college dropouts who would like to come back to a STEM degree. An online degree would be more flexible for their schedules. Therefore, we considered offering the degree online. However, this brought additional challenges in terms of hands-on learning. Some of the IoT courses require working with IoT devices in the lab to program or access them. When the course is offered online, such opportunities will decrease as the students may not have access to these devices.

To mitigate this situation, we designed the courses in such a way that the students can purchase IoT kits or devices to conduct their assignments as if this is replacing the textbooks. For instance, most of the assignments could be done on Raspberry PIs and a Raspberry PI costs about $30-$40 which is even cheaper than a book. Depending on the course, the instructor needs to plan the needed devices as a kit and ask students to buy them. If the assignment requires any demo, such demos could be recorded and submitted along with the assignment. Nevertheless, for group projects this might be a barrier. For instance, for Senior Projects the students will not be able to work as a team unless they live close to each other. For minimizing the impact, we currently offer Senior Design projects that are individual. Obviously, there needs to be more research on how IoT course assignments and projects could be offered online.

5   Other Related Issues

In this section, we discuss other related issues with the new degree.

5.1   Potential Jobs

The graduates of the program can seek employment in any area related to the tech industry including smart homes, smart grid, smart transportation and smart medical devices. The current growth and demand for professionals with the skill sets for developing and implementing IoT will have significant potential for employment locally, statewide, nationally and internationally. In Table 2, we list a categorization of these existing and potential job titles.

5.2   Tracks or Other Joint Programs

Currently, at FIU, we do not offer any tracks or concentrations under the proposed degree but this can be possible in the future as we see more developments and needs. For instance, data analytics with cloud can be a concentration as it has huge potential. Similarly, IoT programming, security and privacy and machine learning could easily become new tracks with the availability of new elective courses.

Table 2. Potential IoT Jobs.

Job Title	Category
IoT Technical Architect	Application
IoT Fog Architect	Application
IoT Consultant	Application
IoT Specialist	Application
IoT Manager	Application
IoT Solutions Architect	Application
IoT Developer	Software
IoT Software Architect	Software
IoT Cloud Architect	Software
IoT Security Analyst	Security/Privacy
IoT Privacy Analyst	Security/Privacy
IoT Data Analyst	Data
IoT Machine Learning Specialist	Data
IoT Policy Advisor	Policy
IoT Compliance Manager	Policy

The other possibility is to consider joint certificates with other majors as IoT is being heavily used in certain areas under non-engineering degrees. For instance, at FIU, we currently started a certificate with School of Hospitality in IoT with a funding from Cisco Silicon Valley Foundation. This program targets up or re-skilling the workforce in Hospitality domain with IoT skills so that they can catch up with the technology. We offer IoT courses in relation to hospitality with applications, compliance and analytics. Some of the courses are offered by School of Hospitality while some more technical courses are used from our own IoT program in Engineering. Similar tracks could be offered in other departments such as Agriculture, Logistics/Supply Chain, Public Administration, Public Health, and Law School. For each of these joint certificates, new courses could be designed.

Finally, the question of where to host the IoT technology degree is relevant. We believe that either Computer Science or Engineering can offer this type of degrees. However, they need to focus on different aspects of IoT. For instance, Computer Science may focus on programming, cloud management, privacy, and machine learning aspects while Computer Engineering may focus on hardware/wireless, low level programming and security. It is important to note that these degrees can be designed either as a technology or engineering degree. In the case of latter, there will be Math and/or Discrete Math requirements and the aim will be on the designing and creation of IoT systems or devices.

6   Conclusion

IoT domain became very mature with a wide range of applications and it is ready to become a dedicated degree. An IoT undergraduate degree can be offered as an engineering or a technology degree as both are needed with the given projections

of IoT applications, devices and jobs. The curriculum choices and requirements will be different depending on the objectives and directions. In addition, IoT degrees can also be tuned to have a flavor in one of the core areas such as hardware, software, etc. depending on where the degree is hosted.

In this paper, we shared our experience in designing the first technology degree in IoT which aimed to attract students who are not necessarily interested in Math/Engineering but still have a passion in technology. The proposed degree not only fills the gap in the changing job market which is being heavily dominated with IoT applications but also to help increase enrollment in STEM areas. The degree can also have a major impact on research by enabling collaboration with IoT industry and other disciplines where fresh students equipped with IoT-related skills could be involved. The online version of the program can also attract non-traditional and international students. We believe that upcoming years will witness an increased number of such IoT degrees and certificates at the undergraduate level.

References

1. T. Qiu, N. Chen, K. Li, M. Atiquzzaman, and W. Zhao, "How can heterogeneous internet of things build our future: A survey," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 3, pp. 2011–2027, 2018.
2. L. Da Xu, W. He, and S. Li, "Internet of things in industries: A survey," *IEEE Transactions on industrial informatics*, vol. 10, no. 4, pp. 2233–2243, 2014.
3. I. Lee and K. Lee, "The internet of things (iot): Applications, investments, and challenges for enterprises," *Business Horizons*, vol. 58, no. 4, pp. 431–440, 2015.
4. R. Bikmetov, M. Y. A. Raja, and T. U. Sane, "Infrastructure and applications of internet of things in smart grids: A survey," in *2017 North American Power Symposium (NAPS)*.   IEEE, 2017, pp. 1–6.
5. M. S. Mekala and P. Viswanathan, "A survey: Smart agriculture iot with cloud computing," in *2017 international conference on microelectronic devices, circuits and systems (ICMDCS)*.   IEEE, 2017, pp. 1–7.
6. "Internet of things (iot) examples," https://www.postscapes.com/internet-of-things-examples.
7. "18 most popular iot devices in 2019," https://www.softwaretestinghelp.com/iot-devices.
8. "Overview of the most popular smart home devices," http://iotlineup.com.
9. F. Samie, L. Bauer, and J. Henkel, "Iot technologies for embedded computing: A survey," in *Proceedings of the Eleventh IEEE/ACM/IFIP International Conference on Hardware/Software Codesign and System Synthesis*.   ACM, 2016, p. 8.
10. H. Hejazi, H. Rajab, T. Cinkler, and L. Lengyel, "Survey of platforms for massive iot," in *2018 IEEE International Conference on Future IoT Technologies (Future IoT)*.   IEEE, 2018, pp. 1–8.
11. O. Vermesan, P. Friess *et al.*, *Internet of things-from research and innovation to market deployment*.   River publishers Aalborg, 2014, vol. 29.
12. E. Ahmed, I. Yaqoob, A. Gani, M. Imran, and M. Guizani, "Internet-of-things-based smart environments: state of the art, taxonomy, and open research challenges," *IEEE Wireless Communications*, vol. 23, no. 5, pp. 10–16, 2016.
13. K. Ashton, *How to fly a horse*.   Larry R. Montgomery, 2015.

14. "Gartner says 5.8 billion enterprise and automotive iot endpoints will be in use in 2020," https://www.gartner.com/en/newsroom/press-releases/2019-08-29-gartner-says-5-8-billion-enterprise-and-automotive-io.
15. "Unlocking opportunities in the internet of things," https://www.bain.com/insights/unlocking-opportunities-in-the-internet-of-things/.
16. "The iot job market: Who's getting hired, and why?" https://internetofthingsrecruiting.com/the-iot-job-market-whos-getting-hired-and-why.
17. "Iot jobs: Get a red-hot career by learning this red-hot skills," http://techgenix.com/hot-iot-jobs.
18. "Intel academic iot course," https://www.youtube.com/playlist?list=PLFBM-eCNdj6A5VSmOEjpn8XoiM88398B7.
19. "Stanford internet of things graduate certificate," https://online.stanford.edu/programs/internet-things-graduate-certificate.
20. "School of internet of things engineering of jiangnan university," http://iot.jiangnan.edu.cn/English/About1/About_us.htm.
21. "College of internet of things engineering of hohai university," http://en.hhu.edu.cn/_t4/2012/1018/c357a606/page.htm.
22. "School of internet of things engineering of xjtlu entrepreneur college," https://www.xjtlu.edu.cn/en/find-a-programme/undergraduate/internet-of-things-engineering.
23. "Iot bachelor's degree at fiu," https://internetofthings.fiu.edu.
24. "Raspberry pi device," https://www.raspberrypi.org/.
25. O. Standard, "Mqtt version 3.1. 1," *URL http://docs. oasis-open. org/mqtt/mqtt/v3*, vol. 1, 2014.
26. C. Bormann, A. P. Castellani, and Z. Shelby, "Coap: An application protocol for billions of tiny internet nodes," *IEEE Internet Computing*, no. 2, pp. 62–67, 2012.